FIDELIS CYBERSECURITY™

CYBERSECURITY IN HEALTHCARE: **A TIME TO ACT**

Why healthcare is especially vulnerable to cyberattacks, and how it can protect data and mitigate risk

At a time of well-publicized incidents of cybersecurity breaches across all industries and government agencies, the healthcare industry—both providers and payers—are especially at risk.

According to the U.S. Department of Health & Human Services Office of Civil Rights, more than 94 million individuals were affected by breaches at healthcare organizations during the first six months of 2015, a 20-fold increase, compared to all of 2014, when 12.5 million individuals were affected. That number was driven up by truly massive incidents. Between January and July of 2015 the top three healthcare breaches alone affected more than 90 million individuals, compared to 7.5 million individuals who were affected by the top three breaches in all of 2014.

In the Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, released in May 2015 by the Ponemon Institute, more than 90 percent of the 90 healthcare organizations and 88 business associates surveyed, reported having a data breach, and 40 percent of those had more than five breaches in the past two years. The average cost of a data breach in healthcare is $2.1 million dollars. For the first time, criminal attacks are the number one cause of a breach in healthcare—up 125 percent compared to five years ago.

According to the Ponemon report, employee negligence was cited as the greatest security incident concern, followed by cyberattacks, use of public cloud services, and mobile device insecurity. Surprisingly, many cyberattacks are decidedly low-tech: lost or stolen devices and spear phishing were cited as the top two security incidents by both healthcare organizations and business associates.

HEALTHCARE: AN ATTRACTIVE TARGET

Beyond the raw numbers, cybersecurity experts point to specific factors that make healthcare payers and providers especially attractive to cyberattack. Larry Ponemon, Ph.D., chairman and founder of the Ponemon Institute, notes that the healthcare record is a treasure trove for cybercriminals. On the black market, a person's social security number and date of birth is worth roughly one dollar. A person's health record, by contrast, is worth between $50 and $70.

One reason for the high demand in the black market of healthcare information is that of continuing value. "A lot of information in the health record doesn't grow stale. All of that information is good to go, and opportunities are going to occur not just once, but many times in a victim's life, so the end result is a pretty valuable piece of information," *said Ponemon.*

Specific examples of the type of information that would not go stale and that are unique to healthcare records, are information about treatments and prescriptions, as well as social security numbers, all of which can be used to commit identity theft. According to the Ponemon benchmark study, medical identity theft nearly doubled in five years, from 1.4 million adult victims to over 2.3 million in 2014.

The Ponemon study found that medical files and billing/insurance records contain the most valuable patient data, which are most often successfully targeted by cybercriminals. Many healthcare organizations recognize the potential harm to patients whose records have been lost or stolen. Seventy-four percent of respondents said there is an increased risk that personal health facts will be disclosed and 65 percent believe that patients who have had their records stolen are more likely to become victims of medical identity theft. Fifty-nine percent of respondents said the risk of financial identity theft increases.

"A lot of information in the health record doesn't grow stale. All of that information is good to go, and opportunities are going to occur not just once, but many times in a victim's life, so the end result is a pretty valuable piece of information."

Larry Ponemon, Ph.D., chairman and founder of the Ponemon Institute

Coupled with the high value of stolen information is laxness within the healthcare industry. IT security at many healthcare organizations, particularly second- and third-tier organizations, is inadequate, Ponemon says. Information sharing between healthcare organizations, which is now mandated by the Affordable Care Act and required for participation in health information exchanges and accountable care organizations, can put all organizations at risk. Those with weak security procedures can serve as a "back door" for hackers, putting other organizations at risk, he says.

Despite the recognition of the risks cited in the Ponemon report, 65 percent of healthcare organizations polled in the survey said they do not offer protection services. Yet that may be changing. In July, for example, the Blue Cross Blue Shield Association announced that beginning Jan. 1, 2016, all Blue Cross and Blue Shield companies will make identity protection services

available to their customers nationwide. The association says that the new protection services will provide heightened safeguards in the event of fraudulent use of personal and financial information for the patients that BCBS companies serve. The offering, which will be available on an opt-in basis, will include credit monitoring, fraud detection, and fraud resolution support.

CHANGING NATURE OF ATTACKS, EMERGING THREATS

George W. McCulloch, Jr., is executive vice president, membership and professional development, at the College of Healthcare Information Management Executives (CHIME) and member of the advisory board of the Association for Executives in Health Information Security. He is also former deputy CIO of Vanderbilt University Hospital System.

The concept of cybersecurity should be front and center at healthcare organizations, he says. He notes that hospital networks are vast, and it is a huge challenge to maintain visibility over the entire network, McCulloch says. "The things I own I can control by having the tools in place and people monitoring what goes on in my organization," he says.

Interconnectivity has added another layer of complexity. "It's the transmission of data that I have to watch. Monitoring access of employees working off-site is also a security challenge, he says. Monitoring third-party vendors is an added challenge. "Do I have business associate agreements? Because their vulnerability is my vulnerability," he says.

Lee Barrett, executive director of the Electronic Healthcare Network Accreditation Commission, says that the complexity of healthcare today, in terms of sharing of health data with other providers, participation in health insurance exchanges and accountable care organizations, use of patient portals and provider portals, has placed new demand on security departments in healthcare organizations. "We have so many connection points and exchange points for data that the risk continues to go up because we now have to control and lock down as many of these points as possible," he says.

> "The things I own I can control by having the tools in place and people monitoring what goes on in my organization."
>
> George W. McCulloch, Jr., Executive Vice President, Membership and Professional Development, at the College of Healthcare Information Management Executives (CHIME)

That complexity needs to be taken into account as organizations put together their security and risk assessment. While securing a network is absolutely getting more expensive, he emphasizes that those expenses must be weighed against the cost of a breach to an organization in terms of lost credibility, lost revenue, and fines.

12 STEPS TO SECURING THE HEALTHCARE ENVIRONMENT

While there are no shortcuts to increasing cybersecurity, experts point to steps organizations can take that are highly effective to securing data and mitigating threats.

1. CONDUCT AN ANNUAL RISK ASSESSMENT: Risk assessments are effective at ensuring organizations have the policies, procedures and controls in place for intrusion detection and penetration testing. Barrett emphasizes that a proactive approach is essential to identifying gaps and putting in appropriate controls and response mechanisms. Once those controls are in place, they need to be monitored constantly.

2. USE INDEPENDENT THIRD-PARTY REVIEW: Use an independent third-party to review the entire infrastructure and make recommendations about potential security gaps and what needs to be done to mitigate those vulnerabilities.

3. BE PREPARED: The key for organizations is to have their plans, policies and procedures in place so they are prepared to deal with a breach when it occurs, both proactively and reactively.

4. EMPHASIZE QUICK DETECTION AND CONTAINMENT: Organizations should implement technologies that detect suspicious or unusual transactions. "We need to move away from the idea that you can have perfect prevention, and emphasize that you can have quick containment," Ponemon says.

> "I think we are going to have a rough go of it. We are still on a learning curve."
>
> George W. McCulloch, Jr., Executive Vice President, Membership and Professional Development, at the College of Healthcare Information Management Executives (CHIME)

5. CENTRALIZE COMMAND AND CONTROL: Appoint one person with the authority to get things done, and provide adequate resources to accomplish his or her goals. Have a crisis team in place to immediately go into "war room" mode at the first evidence that the network defenses have been penetrated, to determine how to contain the threat, determine the extent of the damage, how to report it to the appropriate government agencies, and how to handle the incident from a public-relations perspective.

6. SCRUTINIZE THIRD-PARTY RELATIONSHIPS: While a healthcare organization may have a good handle on its own policies, procedures and controls, it is not necessarily the case for business associates with which they do business. Barrett recommends that a business associate submit to a third-party review so that the vendor meets minimum acceptable requirement.

7. ENCRYPT DATA: Data encryption and tokenization of data (substituting a sensitive data element with a non-sensitive equivalent that has no meaning or value), can make a huge impact and go a long way to creating a more secure infrastructure, according to Ponemon.

8. CONTROL ACCESS: Organizations should put in place a policy of role-based access—who has access to what data in the organization. Role-based access ensures that every employee has access only to what he or she needs to have access to, Barrett says.

9. PROVIDE WORKFORCE TRAINING: Make sure all employees are trained on the basics of security, which is essential to building a strong security culture.

10. COMMUNICATE: Good communication between the security professionals in an organization and the upper management and the board is essential. Barrett recommends that the chief information security officer (CISO) attend board meetings to report on the status on security risk at the organization and the need to put controls in place.

11. USE INDUSTRY STANDARDS FOR GUIDANCE: Industry guidelines from the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO) don't necessarily mitigate all cyberattacks, but do reduce the risk of breaches significantly, according to Ponemon.

12. TAKE OUT AN INSURANCE POLICY: The number of healthcare organizations taking out insurance policies is growing rapidly. "Although it is not an overarching solution, many view insurance as

something in their arsenal that they can count on in the event of a big problem," Ponemon says.

REDEFINING A 'WIN' IN CYBERSECURITY

What constitutes a "win" when it comes to cybersecurity? Barrett acknowledges that the level of sophistication of attacks is increasing, as is the frequency of attacks. Many organizations are getting hundreds of attacks a day. While one preventing intruders from penetrating the network should remain a priority, organizations also need to quickly identify and respond to breaches when they do occur. Failure to do so risks significant monetary costs and damaged reputation to the healthcare organization, no matter its size.

Experts interviewed say that healthcare organizations are in a tough battle for cybersecurity and must be vigilant for the long haul. "I think we are going to have a rough go of it. We are still on a learning curve," McCulloch says. He adds that while healthcare organizations will never be completely safe from attacks, they can take steps to considerably minimize risks.